Formaliser l'anneau des adèles d'un corps global

María Inés de Frutos-Fernández

Imperial College London

Résumé : L'anneau des adèles d'un corps global et son groupe des unités, le groupe des idèles, sont des objets fondamentaux en théorie moderne des nombres. Nous discutons d'une formalisation de leurs définitions dans l'assistant de preuves Lean 3. Comme prérequis, nous avons formalisé les valuations adiques sur les domaines de Dedekind. Nous présentons quelques applications, incluant l'énoncé du théorème principal de la théorie du corps de classes global et une preuve que le groupe des classes d'idéaux d'un corps de nombres est isomorphe à un quotient explicite de son groupe de classes d'idèles.

1. Introduction

La théorie des nombres est la branche des mathématiques qui étudie l'anneau des nombres entiers $\mathbb{Z}$ et son corps de fractions $\mathbb{Q}$, l'ensemble des nombres rationnels. Alors que cette description peut sembler désespérément simple, c'est un domaine riche, impliquant des myriades d'abstractions et techniques.

Considérons par exemple le problème de trouver toutes les solutions entières d'une équation polynomiale à plusieurs variables (une "équation diophantienne"). Peut-être que la plus célèbre de ces équations est $x^n + y^n = z^n$, où n est un entier plus grand que 2. Le dernier théorème de Fermat nous dit que cette équation n'a pas de solutions entières pour lesquelles xyz est non nul. Alors que Fermat a pu énoncer cette conjecture en 1637, sa preuve n'a pas été trouvée jusqu'en 1995, bien que quelques cas particuliers aient été établis plus tôt.

La preuve générale, due à Wiles et Taylor, est construite sur le travail combiné de centaines de mathématiciens qui ont développé pendant les deux derniers siècles une théorie arithmétique riche des courbes elliptiques, des formes modulaires et des représentations de Galois. Le résultat-clef est un cas particulier de la conjecture de Taniyama–Shimura–Weil. Si l'on veut formaliser une preuve complète du dernier théorème de Fermat dans un solveur de théorème, on a d'abord besoin de formaliser tous les ingrédients nécessaires.

Dans cet article, nous formalisons l'anneau des adèles et le groupe des idèles d'un *corps global* (une généralisation du corps $\mathbb{Q}$). Comme conséquence de notre travail, nous pouvons établir le théorème principal de la théorie du corps de classes. La théorie du corps de classes est nécessaire pour la preuve de la conjecture de Taniyama–Shimura–Weil, qui implique le dernier théorème de Fermat. Les adèles et les idèles sont utilisées dans de nombreux domaines de la recherche actuelle, incluant la théorie des formes automorphes et le programme de Langlands, un ensemble ambitieux de conjectures qui ont pour but d'établir des connexions profondes entre la géométrie et la théorie des nombres.

Notre formalisation a été réalisée en utilisant l'assistant de preuves Lean 3 [9]. Au moment d'écrire cet article, le code source est en train d'être intégré à la bibliothèque mathématique de Lean `mathlib`. Nous fournissons un dépôt public [1] contenant la version du code à laquelle il est fait référence dans cet article et la documentation associée [2] au format HTML.

Référence : https://arxiv.org/abs/2203.16344.

Traduction : Denise Vella-Chemla, mai 2022.

1. `https://github.com/mariainesdff/ideles/tree/journal-submission`
2. `https://mariainesdff.github.io/ideles/journal-submission/`

Notons que c'est la première fois que les adèles et les idèles ont été formalisées dans un assistant de preuves.

Avant de décrire notre formalisation, nous donnons un rapide survol de l'anneau des adèles de $\mathbb{Q}$. Quand on étudie les nombres rationnels, à la fois des méthodes algébriques et des méthodes analytiques peuvent être utilisées. Une manière naturelle de faire de l'analyse sur $\mathbb{Q}$ est de le voir comme un sous-espace des nombres réels $\mathbb{R}$, qui sont par définition la complétion de $\mathbb{Q}$ selon la valeur absolue habituelle. Pourtant, ce n'est pas la seule valeur absolue qui peut être définie sur $\mathbb{Q}$: en fait, pour tout nombre premier p, il y a une valeur absolue p-adique $|\cdot|_p$ et on peut considérer la complétion correspondante $\mathbb{Q}_p$ de $\mathbb{Q}$. Le théorème d'Ostrowki nous dit que, à une équivalence près, il n'y a pas d'autres valeurs non triviales des nombres rationnels.

On remarque qu'alors que le corps $\mathbb{Q}_p$ des nombres p-adiques est un objet de base en théorie des nombres, il n'a été formalisé dans aucun assistant de preuves jusqu'à 2015, quand Pelayo, Voevodsky, et Warren l'ont formalisé dans la bibliothèque de Coq Unimath [15]. Les nombres p-adiques ont été ajoutés à la bibliothèque mathématique de Lean `mathlib` en 2018, par R. Y. Lewis [12].

Puisque les valeurs absolues différentes sur $\mathbb{Q}$ nous fournissent différentes connaissances à propos des rationnels, une question naturelle est de savoir s'il est possible de les étudier toutes simultanément. Une première approximation consisterait à considérer le produit des complétions selon chaque valeur absolue. Pourtant, pour des raisons techniques, il est mieux de travailler avec le sous-ensemble suivant du produit :

$$\mathbb{A}_{\mathbb{Q}} := \prod_p{}' \mathbb{Q}_p \times \mathbb{R} := \left\{ ((x_p)_p, r) \in \prod_p \mathbb{Q}_p \times \mathbb{R} \;\middle|\; |x_p|_p \leq 1 \text{ pour tous les } p \text{ sauf un nombre fini} \right\}.$$

$\mathbb{A}_{\mathbb{Q}}$ est un anneau selon l'addition et la multiplication terme à terme, il contient $\mathbb{Q}$ comme un sous-anneau via l'application diagonale $r \mapsto ((r)_p, r)$, et il peut être muni d'une topologie qui l'envoie dans un anneau topologique localement compact. On appelle $\mathbb{A}_{\mathbb{Q}}$ l'anneau des adèles ou anneau adélique de $\mathbb{Q}$ et $\mathbb{A}_{\mathbb{Q},f} := \prod_p{}' \mathbb{Q}_p$ son anneau adélique fini. Les groupes des unités de ces anneaux sont respectivement appelés le groupe idélique $\mathbb{I}_{\mathbb{Q}}$ et le groupe idélique fini $\mathbb{I}_{\mathbb{Q},f}$ de $\mathbb{Q}$.

Les définitions de l'anneau adélique et du groupe idélique peuvent être généralisées à n'importe quel corps global K [2] ; voir les sections 3 et 4 pour des détails. Les corps globaux sont l'un des principaux sujets d'étude en théorie algébrique des nombres et ils peuvent être de deux sortes : les corps de nombres, qui sont des extensions finies du corps $\mathbb{Q}$, et les corps de fonctions, qui sont des extensions finies du corps $\mathbb{F}_q(t)$ des fonctions rationnelles sur un corps fini $\mathbb{F}_q$.

Tout corps global est le corps de fractions d'un domaine de Dedekind, mais l'inverse n'est pas vrai. Pourtant, la définition de l'anneau adélique fini a du sens pour tout domaine de Dedekind, et par conséquent, nous l'avons formalisée à ce degré de généralité.

1.1. Lean et mathlib

Lean 3 est un langage de programmation fonctionnel et un assistant de preuves de théorèmes interactif [9] basé sur la théorie des types dépendants, avec non-pertinence de preuve et univers non-cumulatifs [7]. Pour une introduction à Lean, voir par exemple [3].

Ce projet est basé sur la bibliothèque mathématique de Lean `mathlib`, qui est caractérisée par sa nature décentralisée avec plus de 300 contributeurs. À cause de l'organisation distribuée de `mathlib`, il est impossible de citer tous les auteurs qui ont contribué à une portion de code que nous utilisons.

Pourtant, on remarque que notre formalisation fait un usage extensif de la théorie des domaines de Dedekind [4] et de la théorie des espaces uniformes et des complétions, originellement développées dans le projet de formalisation des espaces perfectoïdes [6].

Dans la bibliothèque au cœur de Lean et dans `mathlib`, des classes de type sont utilisées pour gérer les structures mathématiques sur les types. Par exemple, la classe de type `anneau` englobe deux opérations, l'addition et la multiplication, ainsi qu'une liste de propriétés qu'elles doivent satisfaire. Alors, étant donné un type `R`, on peut déclarer une instance `[ring R]`, et la procédure de résolution des instances de Lean en infèrera que `R` a une structure d'anneau.

Outre `instance`, dont nous venons juste de décrire le comportement, nous utilisons dans cet article les mots-clefs `variables`, `def`, `lemma` et `theorem`, qui ont leur sens évident.

1.2. Structure de l'article

Nous commençons la Section 2 avec des rappels basiques sur les domaines de Dedekind et sur leurs valeurs absolues non-archimédiennes, que nous utilisons alors pour définir l'anneau adélique fini et le groupe idélique fini et nous explorons comment ce dernier est relié au groupe des idéaux fractionnels inversibles. En Section 3, nous nous appuyons sur ce travail pour définir l'anneau adélique, le groupe idélique et le groupe des classes d'idèles d'un corps de nombres, alors qu'en Section 4 nous traitons le cas des corps de fonctions. En Section 5 nous discutons de deux applications du groupe idélique à la théorie du corps de classes. Finalement, nous concluons en Section 6 avec quelques remarques au sujet de l'implémentation et une discussion des travaux futurs en lien avec ce projet.

2. L'anneau adélique fini d'un domaine de Dedekind

2.1. Les domaines de Dedekind et les valuations adiques

Il y a plusieurs définitions équivalentes pour les domaines de Dedekind, trois d'entre elles ayant été formalisées dans `mathlib` [4]. Nous travaillons avec celle formalisée dans `is_dedekind_domain` : un domaine de Dedekind R est un domaine intégral noethérien intégralement fermé de dimension de Krull 0 ou 1 [14].

Un domaine de Dedekind de dimension de Krull 0 est un corps. Dans ce projet, on ne considèrera que les domaines de Dedekind de dimension de Krull 1, pour lesquels les idéaux maximaux sont exactement les idéaux premiers non nuls. Quelques exemples de tels domaines sont les entiers relatifs $\mathbb{Z}$, les entiers Gaussiens $\mathbb{Z}[i]{:=}\{a+bi \mid a, b \in \mathbb{Z}\}$, ou l'anneau des polynômes à une seule variable $k[X]$ sur un corps k. Tous ces exemples sont des domaines à factorisation unique ; pourtant, tout domaine de Dedekind n'a pas forcément cette propriété. Par exemple, $\mathbb{Z}[\sqrt{-5}]{:=}\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ est un domaine de Dedekind mais ce n'est pas un domaine à factorisation unique, puisque des éléments comme $6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$ admettent deux factorisations véritablement distinctes.

Le spectre maximal de R est l'ensemble de ses idéaux maximaux (implementé comme un type en Lean). Le corps de fractions K de R est le plus petit corps contenant R ; ses éléments peuvent être représentés par des fractions r/s, où r et s sont dans R et s est non nul. Par exemple, les corps de fractions de $\mathbb{Z}$, $\mathbb{Z}[i]$, et $k[X]$ sont respectivement $\mathbb{Q}$, $\mathbb{Q}(i){:=}\{a + bi \mid a, b \in \mathbb{Q}\}$, et le corps $k(X)$ des fonctions rationnelles sur k.

```
variables (R : Type*) [comm_ring R] [is_domain R] [is_dedekind_domain R]
    {K : Type*} [field K] [algebra R K] [is_fraction_ring R K]
– Note : not the maximal spectrum if R is a field
def maximal_spectrum := {v : prime_spectrum R // v.val ≠ 0}
variable (v : maximal_spectrum R)
```

Soit R un domaine de Dedekind (de dimension de Krull 1). Alors tout idéal non nul de R peut s'écrire comme un produit d'idéaux maximaux, et sa factorisation est unique à réordonnancement près. En particulier, étant donné un élément $r \in R$ et un idéal maximal v de R, on peut compter combien de fois v apparaît dans la factorisation de l'idéal principal (r), et cela définit une valuation additive non-archimédienne sur R [10, Chap II], c'est-à-dire une fonction $\mathrm{val}_v : R \to \mathbb{Z} \cup \{\infty\}$ telle que

1. $\mathrm{val}_v(r) = \infty$ si et seulement si $r = 0$,
2. $\mathrm{val}_v(rs) = \mathrm{val}_v(r) + \mathrm{val}_v(s)$ pour tout r, s dans R, et
3. $\mathrm{val}_v(r + s) \geq \min\{\mathrm{val}_v(r), \mathrm{val}_v(s)\}$ pour tout r, s dans R.

La fonction val_v est appelée la valuation v-adique sur R. Elle peut être étendue à une valuation sur le corps des fractions K de R en définissant $\mathrm{val}_v(r/s) := \mathrm{val}_v(r) - \mathrm{val}_v(s)$. Par exemple, quand $R = \mathbb{Z}$ et $v = (p)$ est l'idéal engendré par un nombre premier, val_v est la valuation p-adique sur $\mathbb{Z}$ et $\mathbb{Q}$.

Pour des raisons à la fois théoriques et d'implémentation, il est plus pratique de travailler avec la version multiplicative de la valuation : étant donné un nombre réel quelconque $n_v > 1$, on définit une fonction $|\cdot|_v : R \to n_v^{\mathbb{Z} \cup \{-\infty\}} = n_v^{\mathbb{Z}} \cup \{0\}$ envoyant r sur $n_v^{-\mathrm{val}_v(r)}$. De la définition de val_v, on déduit immédiatement que $|\cdot|_v$ a les propriétés suivantes :

1. $|r|_v = 0$ si et seulement si $r = 0$,
2. $|rs|_v = |r|_v |s|_v$ pour tout r, s dans R, et
3. $|r + s|_v \leq \max\{|r|_v, |s|_v\}$ pour tout r, s in R.

Une fonction $|\cdot|_v$ satisfaisant les conditions (1) – (3) est appelée une valeur absolue non-archimédienne (notons que la troisième condition est plus forte que $|r + s|_v \leq |r|_v + |s|_v$). Le choix de n_v utilisé dans la définition n'est pas pertinent, au sens où n'importe quels deux choix de n_v amèneront des valeurs absolues équivalentes. Si, au lieu de la propriété (3), la fonction $|\cdot|_v$ satisfait la condition plus faible $|r + s|_v \leq |r|_v + |s|_v$, nous disons que c'est une valeur absolue archimédienne.

Nous formalisons la valeur absolue v-adique sur R en `mathlib` en utilisant la structure `valuation`, qui consiste en une fonction $|\cdot|$ d'un anneau R vers une `linear_ordered_comm_monoid_with_zero` Γ_0 satisfaisant les conditions (2) et (3), plus $|0| = 0$ et $|1| = 1$.

On choisit Γ_0 égal à `with_zero (multiplicative ℤ)`, qui est une façon de représenter $n_v^{\mathbb{Z}} \cup \{0\}$ en Lean. On a utilisé `associates.mk` plutôt que de travailler directement avec des idéaux simplement parce que la factorisation correspondante API était plus pratique.

```
def int_valuation_def (r : R) : with_zero (multiplicative ℤ) :=
ite (r = 0) 0 (multiplicative.of_add (-(associates.mk v.val.val).count
    (associates.mk (ideal.spanr : ideal R)).factors : ℤ))
def int_valuation (v : maximal_spectrum R) :
valuation R (with_zero (multiplicative ℤ)) :=
{    to_fun := v.int_valuation_def,
     map_zero' := int_valuation.map_zero' v,
     map_one'  := int_valuation.map_one' v,
     map_mul'  := int_valuation.map_mul' v,
     map_add'  := int_valuation.map_add' v }
```

On a étendu la `int_valuation` à une `valuation` sur le corps de fractions K, en définissant la valuation d'une fraction comme étant la valuation du numérateur divisée par la valuation du dénominateur. On a vérifié par `lemma valuation_well_defined` que cette définition ne dépend pas du choix de la fraction utilisée pour représenter un élément de K.

```
def valuation_def (x : K) : (with_zero (multiplicative Z)) :=
let s := classical.some (classical.some_spec (is_localization.mk'_surjective
    (non_zero_divisors R) x)) in
    (v.int_valuation_def (classical.some (is_localization.mk'_surjective
    (non_zero_divisors R) x)))/(v.int_valuation_def s)
lemma valuation_well_defined {r r' : R} {s s' : non_zero_divisors R}
     (h_mk : is_localization.mk' K r s = is_localization.mk' K r' s') :
     (v.int_valuation_def r)/(v.int_valuation_def s) =
     (v.int_valuation_def r')/(v.int_valuation_def s')
```

On a prouvé quelques propriétés de la valuation, dont on remarque que pour tout idéal maximal v de R, il existe un uniformisateur $\pi_v \in K$ pour la valuation v-adique, c'est-à-dire un élément ayant $|\pi_v|_v = n_v^{-1}$ pour valeur absolue, ou de façon équivalente, ayant une valuation additive v-adique égale à 1.

```
lemma valuation_exists_uniformizer :
    ∃ (π : K), v.valuation_def π = multiplicative.of_add(-1 : ℤ)
```

Puisque $|\cdot|_v$ est une valeur absolue sur le domaine de Dedekind R et son corps de fractions K, on peut compléter R et K selon $|\cdot|_v$. On dénote les complétions respectives par R_v et K_v, et on rappelle que R_v est un domaine intégral avec K_v comme corps de fractions.

On formalise d'abord la définition de K_v en utilisant la théorie des complétions des corps valués à disposition dans `mathlib`, cette théorie a été développée à l'origine comme une partie de la formalisation des espaces perfectoïdes [6]. Parmi les façons possibles de définir K_v, on a choisi celle-ci à cause de son API puissante : on peut utiliser l'instance `field_completion` pour retrouver le fait que K_v est un corps, et `valued.extension_valuation` pour étendre la valuation v-adique sur K à une valuation sur la complétion K_v.

```
def v_valued_K (v : maximal_spectrum R) : valued K :=
  { Γ₀ := (with_zero (multiplicative ℤ)),
    grp := infer_instance,
    v := v.valuation }
```

```
def K_v := @uniform_space.completion K (us' v)
instance : field (K_v K v) := @field_completion K _ (us' v) (tdr' v) _ (ug' v)
instance valued_K_v : valued (K_v K v) :=
  { Γ₀:= with_zero (multiplicative ℤ),
    grp := infer_instance,
    v := @valued.extension_valuation K _ (v_valued_K v) }
```

On peut montrer que R_v est égal à l'anneau des entiers de K_v, c'est-à-dire le sous-anneau de K_v consistant en les éléments de valeur absolue inférieure ou égale à 1. Dans notre formalisation, nous utilisons effectivement cette caractérisation pour définir R_v, de telle façon que nous avons automatiquement une inclusion de R_v dans K_v.

```
def R_v : subring (K_v K v) :=
@valuation.integer (K_v K v) (with_zero (multiplicative       ℤ)) _ _ (valued_K_v
v).v
```

2.2. L'anneau adélique fini

Maintenant qu'on a défini les valeurs absolues non-archimédiennes sur un domaine de Dedekind R et leur extension à K, on peut tenter de les étudier toutes simultanément. Dans le but de faire cela, on définit l'anneau adélique fini $\mathbb{A}_{R,f}$ de R comme le produit restreint des complétions K_v selon leur anneau d'entiers R_v, i. e.,

$$\mathbb{A}_{R,f} := \prod_v{}' K\_v := \left\{ (x_v)_v \in \prod_v K\_v \;\middle|\; x_v \in R\_v \text{ pour tous sauf un nombre fini de } v \right\},$$

où v parcourt l'ensemble des idéaux maximaux de R. Rappelons que $x_v \in R_v$ est équivalent à $|x_v|_v \leq 1$, de telle façon que $\mathbb{A}_{R,f}$ est une généralisation immédiate de $\mathbb{A}_{\mathbb{Q},f}$.

Puisque $\mathbb{A}_{R,f}$ est un sous-ensemble du produit $\prod_v K_v$, il est facile de démontrer que c'est un anneau commutatif avec addition par composantes terme à terme et multiplication (on a juste besoin de vérifier qu'il est fermé par addition, négation et multiplication).

```
def K_hat := ((v : maximal_spectrum R), (K_v K v))
def finite_adele_ring' := { x : (K_hat R K)  //  ∀ᶠ (v : maximal_spectrum R) in
   filter.cofinite, (x v  R_v K v) }
instance : comm_ring (finite_adele_ring' R K) := ...
```

On munit $\mathbb{A}_{R,f}$ de la topologie engendrée par l'ensemble

$$\{\Pi_v U_v \mid U_v \text{ est ouvert et } U_v = R_v \text{ pour presque tous les } v\}$$

et on prouve que l'addition et la multiplication sur $\mathbb{A}_{R,f}$ sont continues pour cette topologie, ce qui fait de $\mathbb{A}_{R,f}$ un anneau topologique. Bien que ces démonstrations ne soient pas difficiles conceptuellement, leur formalisation s'est avérée assez longue.

```
def finite_adele_ring'.generating_set : set (set (finite_adele_ring' R K)) :=
{U : set (finite_adele_ring' R K) |
    ∃ (V : Π (v : maximal_spectrum R), set (K_v K v)),
        (∀ x : finite_adele_ring' R K, x  U  ∀ v, x.val v  V v) ∧
        (∀ v, is_open (V v)) ∧ ∀ᶠ v in filter.cofinite, V v = R_v K v}
instance : topological_space (finite_adele_ring' R K) :=
topological_space.generate_from (finite_adele_ring'.generating_set R K)
```

Pour tout élément $k \in K$, il y a un nombre fini d'idéaux maximaux v de R tels que la valeur absolue v-adique de k est plus grande que 1 ; Par conséquent, $(k)_v$ est une adèle finie de R. L'application $\text{inj}_K : K \to \mathbb{A}_{R,f}$ qui envoie k sur $(k)_v$ est un homomorphisme injectif d'anneaux, ce qui nous permet de voir K comme un sous-anneau de $\mathbb{A}_{R,f}$.

```
def inj_K : K → finite_adele_ring' R K :=
λ x, ⟨(λ v : maximal_spectrum R, (coe : K → (K_v K v)) x), inj_K_image R K x⟩
```

On peut se demander pourquoi on a défini $\mathbb{A}_{R,f}$, plutôt que de juste travailler avec le produit complet $\prod_v K_v$. La raison principale à cela est que, alors qu'à la fois $\mathbb{A}_{R,f}$ et $\prod_v K_v$ sont des anneaux topologiques contenant K comme sous-anneau, seul le premier est localement compact et contient K comme sous-anneau discret et co-compact. Puisque $\mathbb{A}_{R,f}$ est en particulier un groupe topologique localement compact, il est possible de définir une mesure de Haar (unique aux scalaires près) sur $\mathbb{A}_{R,f}$, qui nous permet d'intégrer les fonctions sur $\mathbb{A}_{R,f}$. Tate a utilisé cette théorie de l'intégration d'une façon célèbre dans sa thèse pour étudier les propriétés des L-fonctions de Hecke des corps de nombres. Notons que les mesures de Haar ont récemment été formalisées dans `mathlib` [17].

2.2.1. Une définition alternative de l'anneau adélique fini

Il y a une seconde caractérisation de l'anneau des adèles finies de R qui est également largement utilisée en théorie des nombres. On commence avec le produit $\widehat{R} := \prod_v R_v$ sur tous les idéaux maximaux de R et on observe qu'il contient R via l'inclusion diagonale $r \mapsto (r)_v$. Par conséquent, on peut considérer la localisation $(\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$ de $\widehat{R}$ en $R \setminus \{0\}$, constituée des tuples de la forme $(\frac{r_v}{s})_v$ où $r_v \in R_v$ pour tout v et $s \in R \setminus \{0\} \subseteq R_v \setminus \{0\}$.

Pour définir la structure topologique d'anneau sur $\widehat{R}[\frac{1}{R\setminus\{0\}}]$, on utilise le fait que pour tout anneau S, les topologies d'anneau sur S forment un treillis complet. En particulier, étant donnée n'importe quelle application $f : T \to S$ d'un espace topologique T à un anneau S, on peut définir la topologie co-induite sur S comme étant la plus fine topologie telle que S est un anneau topologique et f est continue. La structure de treillis complet a été formalisée comme partie de ce projet et fait déjà partie de `mathlib`.

On donne à $\widehat{R}[\frac{1}{R\setminus\{0\}}]$ la topologie d'anneau co-induite par l'application de localisation $(r_v)_v \mapsto (\frac{r_v}{1})_v$ de $\widehat{R}$ avec la topologie produit vers $\widehat{R}[\frac{1}{R\setminus\{0\}}]$.

Il est bien connu que $\mathbb{A}_{R,f}$ est isomorphe à $(\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$ comme anneaux topologiques. Étant donné un élément $(\frac{r_v}{s})_v \in (\prod_v R_v)[\frac{1}{R\setminus\{0\}}]$, la valeur absolue $|\frac{r_v}{s}|_v$ sera inférieure ou égale à 1, excepté possiblement sur les v en nombre fini qui divisent le dénominateur s ; par conséquent, $(\frac{r_v}{s})_v$ est une adèle finie et on peut facilement voir que cette application est un isomorphisme d'anneaux. Vérifier que c'est également un homéomorphisme nécessite davantage de travail.

On formalise cette seconde définition de l'anneau adélique dans `finite_adele_ring`, mais on omet pour l'instant la formalisation de la démonstration que les deux définitions amènent à des anneaux topologiques isomorphes. La définition `finite_adele_ring` présente l'avantage que, étant définie comme une localisation, `finite_adele_ring R` hérite automatiquement d'une structure d'anneau topologique commutatif, alors que pour `finite_adele_ring' R` cela doit être prouvé à la main. Pourtant, on a trouvé que pour prouver des résultats tels que celui décrit en Section 5.1, il était plus facile de travailler avec notre première définition.

```
def finite_adele_ring := localization (diag_R R K)
instance : comm_ring (finite_adele_ring R K) := localization.comm_ring
instance : algebra (R_hat R K) (finite_adele_ring R K) := localization.algebra
instance : is_localization (diag_R R K) (finite_adele_ring R K):=
localization.is_localization
instance : topological_space (finite_adele_ring R K) :=
localization.topological_space
instance : topological_ring (finite_adele_ring R K) :=
localization.topological_ring
```

2.3. Le groupe idélique fini

Le groupe idélique fini $\mathbb{I}_{R,f}$ de R est le groupe des unités de l'anneau fini adélique $\mathbb{A}_{R,f}$.

C'est un groupe topologique avec la topologie induite par l'application $\mathbb{I}_{R,f} \to \mathbb{A}_{R,f} \times \mathbb{A}_{R,f}$ envoyant x sur (x, x^{-1}).

```
def finite_idele_group' := units (finite_adele_ring' R K)
instance : topological_space (finite_idele_group' R K) := units.topological_space
instance : group (finite_idele_group' R K) := units.group
instance : topological_group (finite_idele_group' R K) := units.topological_group
```

Notons que pour tout $k \in K$ non nul, l'adèle finie $(k)_v$ est inversible, d'inverse $(k^{-1})_v$. Il s'ensuit de cela que $\mathbb{I}_{R,f}$ contient $K^* = K \setminus \{0\}$ comme sous-groupe. On formalise ce fait en définissant une fonction `inj_units_K` de K^* dans $\mathbb{I}_{R,f}$ et en démontrant que c'est un homomorphisme injectif de groupes.

```
def inj_units_K : units K → finite_idele_group' R K :=
λ x, ⟨ inj_K R K x.val, inj_K R K x.inv, right_inv R K x, left_inv R K x ⟩
```

2.4. Relation aux idéaux fractionnaires

Le groupe fini des idèles de R est très relié à son groupe d'idéaux fractionnaires inversibles. Un idéal fractionnaire de R est un R-sous-module I de K pour lequel il existe un $a \in R$ tel que aI est un idéal J de R. On dit que I est inversible s'il existe un autre idéal fractionnaire I' tel que $II' = R$.

Pour un domaine de Dedekind R, tout idéal fractionnaire est inversible et peut être factorisé comme une produit $v_1^{n_1} \cdots v_m^{n_m}$ d'idéaux maximaux de R où les n_i sont des entiers, de façon unique à réordonnancement des facteurs près. On formalise cette définition dans `fractional_ideal.factorization`, où on exprime I comme un `finprod` sur tous les idéaux maximaux de R. On fournit également quelques API pour travailler avec les exposants apparaissant dans cette factorisation.

```
lemma fractional_ideal.factorization (I : fractional_ideal (non_zero_divisors R)
K)
    (hI : I ≠ 0) {a : R} {J : ideal R}
    ( haJ : I = fractional_ideal.span_singleton (non_zero_divisors R)
      ((algebra_map R K) a)⁻¹* ↑ J) :
    Π^f (v : maximal_spectrum R),
      (v.val.val : fractional_ideal (non_zero_divisors R) K)^ ((associates.mk
      v.val.val).count (associates.mk J).factors - (associates.mk v.val.val).count
      (associates.mk (ideal.span{a})).factors : ℤ) = I
```

On peut définir un homomorphisme de groupe de $\mathbb{I}_{R,f}$ vers le groupe des idéaux fractionnaires inversibles en envoyant $(x_v)_v \in \mathbb{I}_{R,f}$ vers le produit $\Pi_v v^{\mathrm{val}_v(x_v)}$. Puisque pour tout $(x_v)_v \in \mathbb{I}_{R,f}$ il y a un nombre fini d'idéaux maximaux v tels que $\mathrm{val}_v(x_v)$ est non nul, ce produit est effectivement fini, et par conséquent il définit en effet un idéal fractionnaire non nul de R.

```
def finite_idele.to_add_valuations (x : finite_idele_group' R K) :
     (v : maximal_spectrum R), ℤ := λ v, -(with_zero.to_integer
      ((valuation.ne_zero_iff valued.v).mpr (v_comp.ne_zero R K v x)))
lemma finite_add_support (x : finite_idele_group' R K ) :
    ∀^f (v : maximal_spectrum R) in filter.cofinite,
      finite_idele.to_add_valuations R K x v = 0 := ...
def map_to_fractional_ideals.val :
    (finite_idele_group' R K) → (fractional_ideal (non_zero_divisors R) K) :=
λ x, Π^f (v : maximal_spectrum R), (v.val.val : fractional_ideal
    (non_zero_divisors R) K)^ (finite_idele.to_add_valuations R K x v)
```

On montre que cet homomorphisme est surjectif et que son noyau est l'ensemble $\mathbb{I}_{R,\infty}$ des éléments $(x_v)_v$ dans $\mathbb{I}_{R,f}$ ayant une valuation additive nulle en tous les v. Pourtant, cette application est

continue quand on donne au groupe des idéaux fractionnaires inversibles la topologie discrète.

3. Adèles et idèles des corps de nombres

3.1. Corps de nombres et leurs anneaux d'entiers

Un corps de nombres K est une extension finie du corps $\mathbb{Q}$ des nombres rationnels [10]. Toute extension finie est algébrique, et donc tout élément $k \in K$ est la racine d'un polynôme à coefficients dans $\mathbb{Q}$. Si de plus k est la racine d'un polynôme unitaire à coefficients entiers, on dit que k est un entier algébrique. Les entiers algébriques de K forment un sous-anneau $\mathcal{O}_K$, appelé l'anneau des entiers de K, qui est un domaine de Dedekind de dimension de Krull 1 dans lequel tout idéal non nul est d'indice fini.

Rappelons de l'introduction qu'une motivation pour définir les adèles de K était à la fois d'étudier simultanément toutes les (classes d'équivalence des) valeurs absolues non-triviales sur K. Ces valeurs absolues peuvent être séparées en deux sortes : les non-archimédiennes et les archimédiennes. Les non-archimédiennes sont exactement les valeurs absolues v-adiques associées aux idéaux maximaux de l'anneau des entiers $\mathcal{O}_K$, dont il a été question à la section 2.1.

Pour obtenir les valeurs absolues archimédiennes, rappelons d'abord que l'on peut trouver une base d'espace $\mathbb{Q}$-vectoriel de K de la forme $\{1, \alpha, \ldots, \alpha^{n-1}\}$, où n est la dimension de K sur $\mathbb{Q}$ et α est un élément de K. Cet α est une racine d'un polynôme du $n^{\text{ième}}$ degré f_α à coefficients dans $\mathbb{Q}$. Pour chaque racine réelle r de f_α, on obtient un plongement de K dans l'ensemble des nombres réels $\mathbb{R}$ (l'application envoyant α sur r), et en restreignant la valeur absolue habituelle sur $\mathbb{R}$ à l'image de K, on obtient une valeur absolue archimédienne sur K. Similairement, pour toute paire de racines complexes conjuguées (s_1, s_2) de f_α, on obtient une paire de plongements de K dans les nombres complexes $\mathbb{C}$, et on peut restreindre la valeur absolue complexe à l'image de K selon l'une ou l'autre pour obtenir une valeur absolue sur K. Notons que les deux plongements provenant d'une paire conjuguée fournissent des valeurs absolues équivalentes.

3.2. L'anneau des adèles

Soit K un corps de nombres. On définit l'anneau des adèles de K comme le produit restreint des complétions K_v de K selon chaque valeur absolue $|\cdot|_v$ sur lui : $\mathbb{A}_K := \prod'_{|\cdot|_v} K_v$. C'est-à-dire, $\mathbb{A}_K$ est le sous-anneau du produit $\prod_{|\cdot|_v} K_v$ consistant en des tuples $(a_v)_v$ tels que $|a_v|_v \leq 1$ pour tous les v sauf pour un nombre fini d'entre eux.

Puisque toute valeur absolue non-archimédienne $|\cdot|_v$ correspond à un idéal maximal v de O_K, et qu'il y a un nombre fini de valeurs absolues, on peut réécrire cette définition ainsi

$$\mathbb{A}_K := \prod_{v \text{ max.}}{}' K_v \times \prod_{|\cdot|_v \text{ arch.}} K_v = \prod_{v \text{ max.}}{}' K_v \times (\mathbb{R} \otimes_{\mathbb{Q}} K),$$

où on a utilisé un théorème de la théorie des nombres algébriques pour obtenir la seconde égalité. Notons que $\prod'_v K_v$ est l'anneau adélique fini associé au domaine de Dedekind $\mathcal{O}_K$; on le dénotera par $\mathbb{A}_{K,f}$ et on l'appellera l'anneau adélique fini de K. On formalise ces définitions comme suit :

```
variables (K : Type) [field K] [number_field K]
def A_K_f := finite_adele_ring' (ring_of_integers K) K
def A_K := (A_K_f K) ×(ℝ ⊗ [ℚ]K)
```

On a prouvé en Section 2.2 que `A_K_f` est un anneau topologique commutatif. Le produit et le produit tensoriel des anneaux commutatifs étant des anneaux commutatifs, `A_K` est donc un anneau commutatif. Pour prouver que c'est un anneau topologique commutatif, il suffit par conséquent de montrer que $\mathbb{R} \otimes_{\mathbb{Q}} K$ est un anneau topologique.

On fait cela en utilisant le fait qu'il y a des isomorphismes $\mathbb{R}^n \simeq \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}^n \simeq \mathbb{R} \otimes_{\mathbb{Q}} K$, où n est la dimension de K sur $\mathbb{Q}$.

Notons que $\mathbb{R}^n$ est représenté en Lean par le type `fin n → ℝ` des fonctions de $\{1, \ldots, n\}$ vers $\mathbb{R}$, et nous pouvons utiliser `pi` pour obtenir la structure d'anneau topologique comme suit :

```
variables (n : ℕ)
instance : ring (fin n → ℝ) := pi.ring
instance : topological_space (fin n → ℝ) := Pi.topological_space
instance : has_continuous_add (fin n → ℝ) := pi.has_continuous_add'
instance : has_continuous_mul (fin n → ℝ) := pi.has_continuous_mul'
instance : topological_ring (fin n → ℝ) := topological_ring.mk
```

On définit alors la topologie sur $\mathbb{R} \otimes_{\mathbb{Q}} K$ comme la topologie d'anneau co-induite par l'application $\mathbb{R}^n \to \mathbb{R} \otimes_{\mathbb{Q}} K$, où $\mathbb{R}^n$ a la topologie produit.

Finalement, `A_K` devient un anneau topologique avec la topologie produit.

```
def linear_map.Rn_to_R_tensor_K : (fin (finite_dimensional.finrank ℚ K ) → ℝ) →ₗ
     [ℝ] 'ℝ⊗ [ℚ] K )  :=
linear_map.comp (linear_map.base_change K) (linear_map.Rn_to_R_tensor_Qn K)
def infinite_adeles.ring_topology : ring_topology ( ℝ⊗ [ ℚ ] K ) :=
ring_topology.coinduced (linear_map.Rn_to_R_tensor_K K)
instance : topological_space ( ℝ⊗ [ℚ ] K) :=
(infinite_adeles.ring_topology K).to_topological_space
instance : topological_ring ( ℝ⊗ [ ℚ ] K) :=
(infinite_adeles.ring_topology K).to_topological_ring
instance : topological_space (A_K K) := prod.topological_space
instance : topological_ring (A_K K) := prod.topological_ring
```

Nous terminons cette section en rappelant que $\mathbb{A}_{K,f}$ contient le corps K comme un sous-anneau, via l'application diagonale envoyant $k \in K$ sur l'adèle finie $(k)_v$. En combinant ceci avec l'inclusion naturelle $k \mapsto 1 \otimes k$ de K dans $\mathbb{R} \otimes_{\mathbb{Q}} K$, on peut également voir K comme un sous-anneau de $\mathbb{A}_K$.

```
def inj_K_f : K → A_K_fK:= inj_K (ring_of_integers K) K
def inj_K : K→ A_K K :=
λ x, ⟨ inj_K_f K x, algebra.tensor_product.include_right x ⟩
```

3.3. Le groupe des idèles et le groupe des classes d'idèles

On définit le groupe $\mathbb{I}_K$ des idèles de K comme le groupe des unités de l'anneau des adèles $\mathbb{A}_K$, et le groupe $\mathbb{I}_{K,f}$ des idèles finies comme le groupe des unités de $\mathbb{A}_{K,f}$.

```
def I_K_f := units (A_K_f K)
def I_K := units (A_K K)
```

Pour tout $k \in K$ non nul, l'adèle finie $(k)_v$ est une unité (avec inverse $(k^{-1})_v$), et donc est l'adèle $((k)_v, 1 \otimes k)$. Par conséquent, on peut voir K^* comme un sous-groupe du groupe des idèles (finies), ce qui nous permet de définir le groupe des classes d'idèles C_K of K comme le quotient de $\mathbb{I}_K$ par K^* :

```
def C_K := (I_K K) / (inj_units_K.group_hom K).range
```

Le nom de groupe de classes d'idèles est justifié par la proche relation qui existe entre C_K est le groupe des classes d'idèles de K, dont nous discuterons en 5.1.

4. Adèles et idèles de corps de fonctions

Soit k un corps, $k[t]$ est l'anneau des polynômes en une variable sur k et $k(t)$ est le corps des fonctions rationnelles (quotients de polynômes) sur k. Un corps de fonctions F est une extension de corps finie de $k(t)$ [16].

```
variables (k F : Type) [field k] [field F] [algebra (polynomial k) F]
    [algebra (ratfunc k) F] [function_field k F]
    [is_scalar_tower (polynomial k) (ratfunc k) F] [is_separable (ratfunc k) F]
```

Toutes les valeurs absolues qui peuvent être définies sur $k(t)$ sont non-archimédiennes : il y a une valeur absolue v-adique pour chaque idéal maximal v de $k[t]$, plus une valeur absolue supplémentaire, appelée la place à l'infini $|\cdot|_\infty$, définie en posant $\left|\frac{f}{g}\right|_\infty = q^{\deg(f)-\deg(g)}$, où $q > 1$ est un nombre réel fixé. La complétion de $k(t)$ selon cette valeur absolue est le corps $k((t^{-1}))$ des séries de Laurent en t^{-1}.

En suivant la stratégie de la Section 2.1, on formalise $|\cdot|_\infty$ en Lean sous le nom `infty_valuation` et on dénote par `kt_infty` la complétion de $k(t)$ selon $|\cdot|_\infty$.

```
def infty_valuation_def (r : ratfunc k) : with_zero (multiplicative ℤ) :=
ite (r = 0) 0 (multiplicative.of_add ((r.num.nat_degree : ℤ) -
    r.denom.nat_degree))
def kt_infty := @uniform_space.completion (ratfunc k) (usq' k)
```

Plus généralement, toutes les valeurs absolues sur un corps de fonctions F sur k sont non-archimédiennes. La plupart d'entre elles correspondent à des idéaux maximaux de la fermeture algébrique de $k[t]$ dans F. L'anneau des adèles fini de F est le produit restreint

$$\mathbb{A}_{F,f} := \prod_v{}' F_v := \left\{ (x_v)_v \in \prod_v F_v \;\middle|\; |x_v|_v \leq 1 \text{ pour tous les } v \texttt{ sauf un nombre fini d'entre eux} \right\},$$

où v parcourt ces idéaux maximaux. Pourtant, F contient également une collection finie de valeurs absolues non-archimédiennes provenant de la valeur absolue $|\cdot|_\infty$ on $k(t)$. Pour inclure ces valeurs absolues également, on définit l'anneau adélique de F comme le produit

$$\mathbb{A}_F := \mathbb{A}_{F,f} \times (k((t^{-1})) \otimes_{k(t)} F).$$

```
def A_F_f := finite_adele_ring' (ring_of_integers k F) F
def A_F := (A_F_f k F) × ((kt_infty k) ⊗ [ratfunc k] F)
```

L'anneau adélique (fini) de F est un anneau commutatif topologique. On définit le groupe idélique (fini) de F comme étant le groupe des unités, respectivement dénotées par $\mathbb{I}_{F,f}$ et $\mathbb{I}_F$, avec la topologie induite par l'application $x \mapsto (x, x^{-1})$ comme dans la Section 2.3.

Notons qu'en théorie des nombres, on s'intéresse habituellement à l'anneau adélique d'un corps de fonctions sur un corps fini $k = \mathbb{F}_q$. Pourtant, $\mathbb{A}_F$ peut être défini pour tout choix de corps k, de telle façon qu'il n'est pas nécessaire que k soit fini dans notre formalisation. Au lieu de cela, cette assomption de finitude devra être ajoutée dans les lemmes qui la nécessitent.

5. Théorie du corps de classes

La théorie du corps de classes est une branche de la théorie des nombres dont le but est de décrire les extensions abéliennes de Galois d'un corps local ou global K, ainsi que leurs groupes de Galois correspondant, en fonction de l'arithmétique du corps K ([1], [8], [13]). Rappelons de l'introduction qu'un corps global est soit un corps de nombres soit un corps de fonctions sur un corps fini $\mathbb{F}_q$.

Un corps local est la complétion d'un corps global selon une valeur absolue. Des exemples de corps locaux incluent le corps des nombres réels $\mathbb{R}$, le corps des nombres complexes $\mathbb{C}$, les nombres p-adiques $\mathbb{Q}_p$, ou le corps $\mathbb{F}_q((X))$ des séries formelles de Laurent sur un corps fini.

Dans cette section, on discute de deux résultats de la théorie du corps de classes dans lesquels intervient la définition du groupe des classes d'idèles. Le premier résultat est une preuve du fait que le groupe des classes d'idéaux d'un corps de nombres est isomorphe à un quotient de son groupe des classes d'idèles, que nous décrivons explicitement. Le second résultat est une formalisation de

l'énoncé du théorème principal de la théorie du corps de classes global.

5.1. Le groupe des classes d'idéaux est un quotient du groupe des classes d'idèles

Nous avons vu en Section 2.4 que, pour tout domaine de Dedekind R, il y a un homomorphisme de groupes surjectif continu du groupe des idèles finies $\mathbb{I}_{R,f}$ au groupe $\mathrm{Fr}(R)$ des idéaux fractionnaires inversibles de R, envoyant $(x_v)_v$ vers $\prod_v v^{\mathrm{val}_v(x_v)}$.

Si K est un corps de nombres avec anneau des entiers R, on peut étendre cette application à un homomorphisme de groupes $\mathbb{I}_K \to \mathrm{Fr}(R)$ par pré-composition avec la projection naturelle $\mathbb{I}_K \to \mathbb{I}_{K,f}$, obtenant à nouveau une surjection continue. Il est facile de voir qu'une idèle $((x_v)_v, r \otimes_{\mathbb{Q}} k) \in \mathbb{I}_K$ appartient au noyau de cette application, ce que nous dénotons par $\mathbb{I}_{K,\infty}$, si et seulement si $\mathrm{val}_v(x_v)$ est égal à zéro pour tout idéal maximal v de R. Nous avons écrit cette application en Lean et nous avons formalisé les preuves pour chacune des propriétés listées.

```
- For a Dedekind domain R with fraction field K :
def map_to_fractional_ideals.val :
    (finite_idele_group' R K) → (fractional_ideal (non_zero_divisors R) K) :=
λ x, Π^f (v : maximal_spectrum R), (v.val.val : fractional_ideal
    (non_zero_divisors R) K)^ (finite_idele.to_add_valuations R K x v)
```

```
lemma I_K.map_to_fractional_ideals.surjective :
    function.surjective (I_K.map_to_fractional_ideals K) := ...
lemma I_K.map_to_fractional_ideals.continuous :
    continuous (I_K.map_to_fractional_ideals K) := ...
lemma I_K.map_to_fractional_ideals.mem_kernel_iff (x : I_K K) :
    I_K.map_to_fractional_ideals K x = 1 ↔ ∀ v : maximal_spectrum
      (ring_of_integers K), finite_idele.to_add_valuations (ring_of_integers K) K
      (I_K.fst K x) v = 0 := ...
```

Maintenant, nous voulons montrer que cette application induit un homomorphisme au niveau des groupes de classes. Le groupe des classes d'idéaux $\mathrm{Cl}(K)$ de K est défini comme le quotient du groupe des idéaux fractionnaires inversibles de K par le sous-groupe des idéaux fractionnaires principaux. C'est un objet important en théorie algébrique des nombres, puisqu'il peut être interprété comme une mesure de la distance séparant l'anneau des entiers K du fait d'être un domaine de factorisation unique.

Notons que l'idèle $((k)_v, 1 \otimes_{\mathbb{Q}} k)$ correspondant à un $k \in K$ non nul est envoyée vers $\prod_v v^{\mathrm{val}_v(k)}$, qui est l'idéal fractionnaire principal engendré par k. Par conséquent, nous obtenons une application induite du groupe des classes d'idèles C_K vers le groupe des classes d'idéaux $\mathrm{Cl}(K)$. En utilisant la propriété universelle de la topologie quotient, on conclut que cette application $C_K \to \mathrm{Cl}(K)$ est un homomorphisme surjectif continu, ayant $\mathbb{I}_{K,\infty}K^*/K^*$ comme noyau. Par conséquent, par le premier théorème d'isomorphisme pour les groupes topologiques, $\mathrm{Cl}(K)$ est isomorphe au quotient de C_K par $\mathbb{I}_{K,\infty}K^*/K^*$.

En prouvant ce théorème, nous montrons que notre formalisation des adèles et des idèles d'un corps global peut être effectivement utilisée en pratique pour démontrer des résultats de théorie des nombres de niveau universitaire. Alors que nous avons seulement formalisé cette preuve pour les corps de nombres, elle peut être adaptée de façon triviale au cas des corps de fonctions.

5.2. Le théorème principal de la théorie du corps de classes

Soit K un corps de nombres, $\overline{K}$ une clôture algébrique de K et $G_K{:=}\mathrm{Gal}_{\overline{K}/K}$ le groupe de Galois de l'extension $\overline{K}/K$. Le groupe topologique G_K est isomorphe à la limite inverse $\varprojlim_L \mathrm{Gal}(L/K)$ sur toutes les extensions finies L/K, avec la topologie limite inverse. On considère l'abélianisation topologique $G_K^{ab}{:=}G_K/\overline{[G_K, G_K]}$ de G_K, définie comme le quotient de G_K par la fermeture algébrique du sous-groupe commutateur de G_K. Le groupe G_K^{ab} est un groupe topologique avec la topologie quotient, parce que $\overline{[G_K, G_K]}$ est un sous-groupe normal de G_K.

Un exercice en théorie de Galois infinie montre que G_K^{ab} est le groupe de Galois de l'extension abélienne maximale K^{ab} de K. Le théorème principal de la théorie du corps de classe global nous permet de décrire son groupe de Galois en fonction du groupe de classes d'idèles de K :

Théorème [Théorème principal de la théorie du corps de classes global] : *Soit K un corps de nombres. Dénotons par $\pi_0(C_K)$ le quotient de C_K par le composant connexe de l'identité. Il y a un isomorphisme de groupes topologiques $\pi_0(C_K) \simeq G_K^{ab}$.*

On a formalisé l'énoncé de ce théorème en deux parties : on a d'abord stipulé l'existence d'un isomorphisme de groupes `main_theorem_of_global_CFT.group_isomorphism` entre $\pi_0(C_K)$ et G_K^{ab} et alors dans `main_theorem_of_global_CFT.homeomorph` on a énoncé que cette application est également un homéomorphisme. Notons qu'une démonstration complète au papier et stylo occupe des centaines de pages, et nous n'avons donc pas essayé de la formaliser.

```
variables (K : Type) [field K] [number_field K]
theorem main_theorem_of_global_CFT.group_isomorphism : (number_field.C_K K) /
    (subgroup.connected_component_of_one (number_field.C_K K)) ≃* (G_K_ab K) :=
sorry
theorem main_theorem_of_global_CFT.homeomorph :
homeomorph ((number_field.C_K K) / (subgroup.connected_component_of_one
    (number_field.C_K K))) (G_K_ab K) :=
{   continuous_to_fun := sorry,
    continuous_inv_fun := sorry,
    ..(main_theorem_of_global_CFT.group_isomorphism K) }
```

6. Discussion

6.1. Remarques sur l'implémentation

Dans cette section, on discute des détails techniques de notre formalisation. Le premier détail technique a à voir avec l'univers dans lequel le domaine de Dedekind R et son corps de fonctions K sont définis. Pour définir les valuations v-adiques et formaliser les idéaux fractionnaires de factorisation,

on peut poser que R et K sont de `Type u` pour tout univers `u`. Pourtant, pour définir les complétions K_v et tout le travail qui s'ensuit, on a besoin que R et K vivent dans `Type`. Ceci est dû au fait que la structure `valued`, que nous avons utilisée dans nos définitions des complétions, nécessitent que le corps K et le `linear_ordered_comm_monoid_with_zero` Γ_0 vivent dans le même univers, et on a choisi Γ_0 comme étant `with_zero(multiplicative` $\mathbb{Z}$`)`, qui est de type `Type`.

Deuxièmement, on a trouvé que quelques définitions causaient des temps de réponse ou des erreurs de mémoire inattendus, à cause du fait que Lean n'était pas capable de décider si elles étaient calculables ou pas. Nous souhaiterions remercier Gabriel Ebner d'avoir trouvé la cause de ces erreurs et d'avoir fourni la définition `force_noncomputable` pour résoudre ces problèmes, ainsi qu'un lemme `simp` associé.

```
noncomputable def force_noncomputable {α : Sort*} (a : α) : α :=
function.const _ a (classical.choice ⟨ a ⟩)
@[simp] lemma force_noncomputable_def {α} (a : α) : force_noncomputable a = a :=
rfl
```

Comme exemple, la définition de l'application de coertion de $\mathbb{A}_{R,f}$ vers $\prod_v K_v$ a causé une erreur 'excessive memory consumption', qui a été immédiatement résolue par l'application de `force_noncomputable`.

```
def coe' : (finite_adele_ring' R K) → K_hat R K :=
force_noncomputable $ λ x, x.val
```

6.2. Travaux futurs

Il y a plusieurs directions naturelles pour un travail de formalisation futur provenant de ce projet. Nous listons quelques unes d'entre elles, en commençant par les buts les plus immédiats.

- Montrer que les deux définitions de l'anneau adélique fini formalisées en section 2.2 donnent des anneaux topologiques isomorphes. Construire un isomorphisme d'anneaux entre eux deux sera facile, mais vérifier que c'est un homéomorphisme devra nécessiter un certain travail.
- Définir le groupe des classes d'idèles et prouver les résultats de la Section 5.1 dans le paradigme des corps de fonctions. Les preuves seront presque identiques à celles du cas des corps de nombres.
- Formaliser les résultats topologiques à propos de l'anneau adélique et du groupe idélique, tels que la preuve que $\mathbb{A}_K$ est localement compact et contient K comme sous-groupe discret co-compact.
- Plus généralement, avoir les définitions de $\mathbb{A}_K$ et $\mathbb{I}_K$ ouvre la porte à la formalisation de concepts et résultats utilisés dans l'état de l'art de la théorie des nombres, incluant la définition des formes automorphes [5] et l'énoncé de la correspondance de Langlands [11]. Notons que seuls quelques cas de la correspondance de Langlands ont été démontrés, et que le programme de Langlands est actuellement un des domaines de recherche principaux en théorie des nombres.

Bibliographie

[1] Emil Artin and John Tate. *Class Field Theory.* W. A. Benjamin, New York, 1967.

[2] Emil Artin and George Whaples. Axiomatic Characterization of Fields by the Product Formula for Valuations. *Bulletin of the American Mathematical Society*, 51(7) :469 – 492, 1945. URL : https://mathscinet.ams.org/mathscinet-getitem?mr=MR0013145.

[3] Jeremy Avigad, Leonardo de Moura, and Soonho Kong. *Theorem Proving in Lean.* Carnegie Mellon University, 2021. Release 3.23.0. URL : https://leanprover.github.io/theorem_proving_in_lean/.

[4] Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, and Filippo A. E. Nuccio Mortarino Majno di Capriglio. A Formalization of Dedekind Domains and Class Groups of Global Fields. In Liron Cohen and Cezary Kaliszyk, editors, *12th International Conference on Interactive Theorem Proving (ITP 2021)*, volume 193 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 5 :1–5 :19, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL : https://drops.dagstuhl.de/opus/volltexte/2021/13900, doi:10.4230/LIPIcs.ITP.2021.5.

[5] Daniel Bump. *Automorphic Forms and Representations.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1997. doi:10.1017/CBO9780511609572.

[6] Kevin Buzzard, Johan Commelin, and Patrick Massot. Formalising Perfectoid Spaces. In Jasmin Blanchette and Catalin Hritcu, editors, *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*, pages 299–312. ACM, 2020. doi:10.1145/3372885.3373830.

[7] Mario Carneiro. *The Type Theory of Lean.* Springer, Berlin, Heidelberg, 2019. Master thesis. URL : https://github.com/digama0/lean-type-theory/releases.

[8] J. W. S. Cassels and A. Fröhlich (eds.). *Algebraic Number Theory.* Academic Press, London ; Thompson Book Co., Inc., Washington, D.C., 1967.

[9] L. de Moura, S. Kong, J. Avigad, F. van Doorn, and J. von Raumer. The Lean Theorem Prover (System Description). In Felty A. and Middeldorp A., editors, *Automated Deduction - CADE-25*, volume 9195 of *Lecture Notes in Computer Science*, pages 378–388. Springer, Cham, 2015. doi:10.1007/978-3-319-21401-6_26.

[10] Gerald J. Janusz. *Algebraic Number Fields* , volume 55 of *Pure and Applied Mathematics.* Academic Press, London, 2nd edition, 1996.

[11] R. P. Langlands. Problems in the Theory of Automorphic Forms. In *Lectures in Modern Analysis and Applications III*, volume 170 of *Lecture Notes in Mathematics*, pages 18–61. Springer, Berlin, Heidelberg, 1970. doi:10.1007/BFb0079065.

[12] Robert Y. Lewis. A Formal Proof of Hensel's Lemma over the p-Adic Integers. In *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP 2019, page 15–26, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3293880.3294089.

[13] J. S. Milne. Class Field Theory (v4.03), 2020. URL : https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[14] Jürgen Neukirch. *Algebraic Number Theory.* Springer, Berlin, Heidelberg, 1999. doi:10.1007/978-3-662-03983-0.

[15] Álvaro Pelayo, Vladimir Voevodsky, and Michael A. Warren. A univalent formalization of the p-adic numbers. *Mathematical Structures in Computer Science*, 25(5) :1147–1171, 2015. doi:10.1017/S0960129514000541.

[16] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Universitext. Springer, 1993. URL : https://dblp.org/rec/books/daglib/0084861.bib.

[17] Floris van Doorn. Formalized Haar Measure. In Liron Cohen and Cezary Kaliszyk, editors, *12th International Conference on Interactive Theorem Proving (ITP 2021)*, volume 193 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 18 :1–18 :17, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. URL : https://drops.dagstuhl.de/opus/volltexte/2021/13913, doi:10.4230/LIPIcs.ITP.2021.18.